PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 5 :		(11) Internationale Veröffentlichungsnummer: WO 94/06080
G06F 11/08, 11/10, 11/00	A1	(43) Internationales Veröffentlichungsdatum: 17. März 1994 (17.03.94)

(21) Internationales Aktenzeichen: PCT/AT93/00138

(22) Internationales Anmeldedatum: 2. September 1993 (02.09.93)

(30) Prioritätsdaten:
A 1772/92 4. September 1992 (04.09.92) AT

(71) Anmelder *(für alle Bestimmungsstaaten ausser US):* FAULT TOLERANT SYSTEMS [AT/AT]; FTS-Computertechnik GesmbH, Am Bühel 112, A-2500 Baden b. Wien (AT).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US) :* KOPETZ, Hermann [AT/AT]; Am Bühel 112, A-2500 Baden b. Wien (AT).

(74) Anwalt: MATSCHNIG, Franz; Siebensterngasse 54, A-1071 Wien (AT).

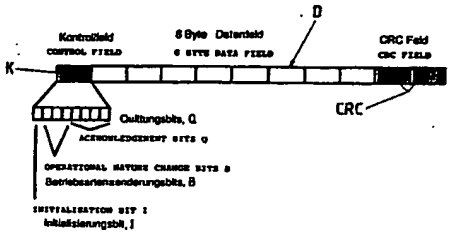
(81) Bestimmungsstaaten: JP, KR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: COMMUNICATIONS CONTROL UNIT AND INFORMATION TRANSMISSION PROCESS

(54) Bezeichnung: KOMMUNIKATIONSKONTROLLEINHEIT UND VERFAHREN ZUR ÜBERMITTLUNG VON NACHRICHTEN

(57) Abstract



A communications control unit and a process for transmitting information within a distributed real-time computer architecture, consisting of a plurality of error-tolerant units in which the information to be transmitted consists of a control field (K), a data field (D) and a CRC (cyclic-redundancy check) field (CRC). The CRC field consists of standard information from the concatenation of the control field (K), the data field (D) and a local internal status of a transmitting communications control unit. The local internal status of such a control unit is provided by the combination of the overall time with a peer field in which to each error-tolerant unit is allocated a given bit, the TRUE status of which indicates correct operation and the FALSE status of which indicates an error status, so that a receiving communications control unit can, by testing an incoming item of data, recognise both incorrect information and a difference between the internal statuses of the transmitting and receiving communications control unit.

(57) Zusammenfassung

Eine Kommunikationskontrolleinheit und ein Verfahren zur Übermittlung von Nachrichten innerhalb einer verteilten Echtzeit- Computerarchitektur, bestehend aus einer Mehrzahl Fehlertoleranter Einheiten, bei welchem die zu übertragenden Nachrichten aus einem Kontrollfeld (K), einem Datenfeld (D) und einem CRC (Cyclic- Redundancy Check) Feld (CRC) zusammengesetzt sind, wobei das CRC-Feld von Standardnachrichten aus der Verkettung des Kontrollfeldes (K), des Datenfeldes (D) und eines lokalen inneren Zustandes einer sendenden Kommunikationskontrolleinheit gebildet wird und sich der lokale innere Zustand einer solchen Kontrolleinheit aus der Verbindung der globalen Zeit mit einem Mitgliedsfeld ergibt, in welchem jeder Fehlertoleranten Einheit ein bestimmtes Bit zugeordnet ist, dessen Zustand WAHR die Funktionstüchtigkeit und dessen Zustand FALSCH einen Fehlerzustand anzeigt, sodaß eine empfangende Kommunikationskontrolleinheit durch Überprüfung einer einlangenden Nachricht sowohl eine fehlerhafte Nachricht, als auch ein Abweichen der inneren Zustände der sendenden und empfangenden Kommunikationskontrolleinheit erkennen kann.

LEDIGLICH ZUR INFORMATION

Code, die zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AT	Österreich	FI	Finnland	MR	Mauritanien
AU	Australien	FR	Frankreich	MW	Malawi
BB	Barbados	GA	Gabon	NE	Niger
BE	Belgien	GB	Vereinigtes Königreich	NL	Niederlande
BF	Burkina Faso	GN	Guinea	NO	Norwegen
BG	Bulgarien	GR	Griechenland	NZ	Neuseeland
BJ	Benin	HU	Ungarn	PL	Polen
BR	Brasilien	IE	Irland	PT	Portugal
BY	Belarus	IT	Italien	RO	Rumänien
CA	Kanada	JP	Japan	RU	Russische Föderation
CF	Zentrale Afrikanische Republik	KP	Demokratische Volksrepublik Korea	SD	Sudan
CG	Kongo	KR	Republik Korea	SE	Schweden
CH	Schweiz	KZ	Kasachstan	SI	Slowenien
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slowakischen Republik
CM	Kamerun	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxemburg	TD	Tschad
CS	Tschechoslowakei	LV	Lettland	TG	Togo
CZ	Tschechischen Republik	MC	Monaco	UA	Ukraine
DE	Deutschland	MG	Madagaskar	US	Vereinigte Staaten von Amerika
DK	Dänemark	ML	Mali	UZ	Usbekistan
ES	Spanien	MN	Mongolei	VN	Vietnam

KOMMUNIKATIONSKONTROLLEINHEIT UND VERFAHREN ZUR ÜBERMITTLUNG VON NACHRICHTEN

Die Erfindung bezieht sich auf eine Kommunikationskontrolleinheit und ein Verfahren zur Übermittlung von Nachrichten innerhalb einer verteilten Echtzeit-Computerarchitektur mit einer gemeinsamen globalen Zeitbasis, bestehend aus einer Mehrzahl Fehlertoleranter Einheiten, welche zumindest je einen fail-silent Computer und je Computer eine Kommunikationskontrolleinheit mit zumindest einem Kommunikationsport aufweisen, wobei jede Fehlertolerante Einheit über zumindest einen Kommunikationskanal mit jeder anderen Fehlertoleranten Einheit verbunden ist und der Zugriff auf den zumindest einen Kommunikationskanal durch ein statisches, von der gemeinsamen globalen Zeitbasis abgeleitetes zyklisches Zeitscheibenverfahren erfolgt.

Die oben genannte, bekannte Computerarchitektur besteht aus einer Anzahl von global synchronisierten fail-silent Computern, die in Fehlertolerante Einheiten zusammengefaßt sind und über ein Broadcastkommunikationssystem Nachrichten austauschen, wobei eine Fehlertolerante Einheit aus zumindest einem fail-silent Computer besteht und jeder Computer eine Kommunikationskontrolleinheit mit mindestens einem Kommunikationsport besitzt. Um den Ausfall eines Computers tolerieren zu können sind häufig zwei aktive Computer, die quasisynchron dieselben Zustandsübergänge vollziehen, zu einer Fehlertoleranten Einheit zusammengefaßt. Das Kommunikationssystem kann z.B. durch den Einsatz von zwei parallelen Kommunikationskanälen redundant ausgelegt sein, wobei jeder Computer über zwei Kommunikationsports der Kommunikationskontrolleinheit an je einen Kanal des Broadcastkommunikationssystems angeschlossen ist. Um auch das Auftreten von hohen transienten Fehlerraten zu beherrschen, kann eine Fehlertolerante Einheit (FTE) neben den beiden aktiv redundanten Computern auch noch einen Schattencomputer beinhalten. Eine solche Architektur ist in Kopetz, H., Kantz, H, Grünsteidl, G, Puschner P, und Reisinger, J, "Tolerating Transient Faults in MARS", Proc. 20th int. Symposium on Fault-Tolerant Computing, IEEE Press, pp., 466 - 473, Juni 1990, genau beschrieben.

Die Übermittlung der Nachrichten erfolgt über ein Verfahren, bei welchem die Zugriffsberechtigung auf die Kommunikationskanäle nach einem statischen Zeitscheibenverfahren von der globalen Zeit abgeleitet wird, sodaß jede Kommunikationskontrolleinheit a priori

weiß, wann eine andere Kommunikationskontrolleinheit eine Nachricht zu senden hat. Jede Kommunikationskontrolleinheit verfügt daher über eine lokale Echtzeituhr, die mit allen anderen Kommunikationskontrolleinheiten innerhalb einer gegebenen Synchronisationsgenauigkeit synchronisiert ist. Ein Verfahren zur Synchronisation der Uhren der Kommunikationskontrolleinheit ist in Kopetz, H., und Ochsenreiter, W., Clock Synchronisation in Distributed Real-Time Systems, IEEE Transactions on Computers, vol c-36, pp. 933 - 940, August 1987, genau beschrieben.

Eine fehlertolerante Echtzeit-Computerarchitektur muß alle Fehlerfälle, die in der Fehlerhypothese spezifiziert sind, nachweislich beherrschen. Zu diesem Zweck sind vom Kommunikationssystem folgende Aufgaben zu erfüllen:

(1) Rechtzeitiger und sicherer Nachrichtenaustausch zwischen den Computern unter Einhaltung der spezifizierten Zeitbedingungen, auch im Fehlerfall.
(2) Erkennung von transienten und permanenten Nachrichtenverlusten.
(3) Konsistente Erkennung vom Computerausfällen.
(4) Verteiltes Redundanzmanagement, d.h. konsistentes Abschalten von fehlerhaften Computern und Zuschalten von reparierten Computern.
(5) Synchronisation der lokalen Uhren.
(6) Schnelle Reaktion in Notsituationen.

Weiters sollen in einem Echtzeitkommunikationssystem die Nachrichtenlänge und die Anzahl der Verwaltungsnachrichten möglichst gering sein, um bei einer gegebenen Bandbreite des Kommunikationskanals eine schnelle Reaktion des Systems zu unterstützen. Eine kurze Nachrichtenlänge und eine geringe Zahl von Verwaltungsnachrichten ist bei schnellen zeitkritischen Prozessen, z.B. in der Automobil- oder Flugzeugelektronik, von großer wirtschaftlicher Bedeutung, da eine Erhöhung der Bandbreite hohe Kosten verursacht.

Gemäß dem Stand der Technik werden die beschriebenen Aufgaben auf unterschiedlichen Ebenen - in Hardware und/oder Software - realisiert, wobei eine Vielzahl zusätzlicher Verwaltungsnachrichten über das Kommunikationssystem zu transportieren ist. Solche Verfahren zur Nachrichtenübermittlung sind beispielsweise unter der Bezeichnung J1850, CAN und Token Slot Network bekannt geworden (1992 SAE Handbook, Vol, pp. 20.301-20.302, Society of Automotive Engineers, 400 Commonwealth Drive, Warrendale, Pa, USA).

Die Erfindung zielt darauf ab, die vorliegenden Aufgaben durch ein integriertes Verfahren in der Hardware der Kommunikationskontrolleinheit zu realisieren, wobei durch Auswertung der a priori Informationen über das Zeitverhalten und der laufenden Information über das Betriebsverhalten des Kommunikationssystems die Anzahl der Verwaltungsnachrichten und die Nachrichtenlänge wesentlich reduziert werden können.

Diese Aufgaben werden erfindungsgemäß durch eine Kommunikationseinheit und ein Verfahren zur Übertragung von Nachrichten gelöst, bei welchem die zu übertragenden Nachrichten aus einem Kotrollfeld, einem Datenfeld und einem CRC (Cyclic Redundancy Check) Feld zusammengesetzt sind, wobei das CRC-Feld von Standardnachrichten, welche durch ein bestimmtes Bit des Kontrollfeldes gekennzeichnet sind, aus der Verkettung des Kontrollfeldes, des Datenfeldes und eines lokalen inneren Zustandes einer sendenden Kommunikationskontrolleinheit gebildet wird und sich der lokale innere Zustand einer solchen Kontrolleinheit aus der Verbindung der globalen Zeit mit einem Mitgliedsfeld ergibt, in welchem jeder Fehlertoleranten Einheit ein bestimmtes Bit zugeordnet ist, dessen Zustand WAHR die Funktionstüchtigkeit und dessen Zustand FALSCH einen Fehlerzustand dieser Fehlertoleranten Einheit anzeigt, sodaß eine empfangende Kommunikationskontrolleinheit durch Überprüfung einer einlangenden Nachricht sowohl eine fehlerhafte Nachricht als auch ein Abweichen der inneren Zustände der sendenden und empfangenden Kommunikationskontrolleinheit erkennen kann.

Weitere Vorteile und Merkmale der Erfindung ergeben sich aus den abhängigen Unteransprüchen und der folgenden Beschreibung eines Ausführungsbeispiels der Erfindung, welche sich auf die beiliegenden Figuren bezieht, die zeigen:

Figur 1 eine schematische Darstellung einer Fehlertoleranten Echtzeit-Computerarchitektur zur Übertragung von Nachrichten,

Figur 2 eine schematische Darstellung des Datenformates der zu übertragenden Nachrichten.

Die Erfindung soll nun anhand des in Figur 1 und 2 dargestellten Ausführungsbeispiels näher erläutert werden. In diesem Beispiel soll der Ausfall einer Nachricht je Übertragung einer Fehlertoleranten Einheit oder der permanente Ausfall einer Kommunikationskontrolleinheit je Fehlertolerante Einheit oder der Ausfall eines kompletten Kommunikationskanals toleriert werden, d.h. es gibt in diesem Beispiel keine Baueinheit, deren Ausfall nicht toleriert wird. Weiters soll in diesem Beispiel zusätzlich zu den zitierten Ausfällen auch noch ein zweiter permanenter oder transienter Fehler durch den Einsatz eines Schatten-

computers toleriert werden. Falls der Ausfall mehrerer Nachrichten toleriert werden soll, so sind die Nachrichten mehrfach zu senden.

Es sei die in Fig. 1 angeführten Konfiguration mit 4 Fehlertoleranten Einheiten FTE_1 FTE_2 FTE_3 FTE_4 mit jeweils zwei aktiven Computern AC_{1a}, AC_{1b}, AC_{2a}, AC_{2b}, AC_{3a}, AC_{3b}, AC_{4a}, AC_{4b} und je einem Schattencomputer SC_1, SC_2, SC_3, SC_4 gegeben. Jede Kommunikationskontrolleinheit KE_{1a}, KE_{1b}, KE_{1c}, KE_{2a}, KE_{2b}, KE_{2c}, KE_{3a}, KE_{3b}, KE_{3c}, KE_{4a}, KE_{4b}, KE_{4c} ist über zwei Kommunikationskanäle KK_1, KK_2 mit jeder anderen Kommunikationskontrolleinheit verbunden und verfügt über eine lokale Echtzeituhr, die mit allen anderen Kommunikationskontrolleinheiten innerhalb einer gegebenen Synchronisationsgenauigkeit synchronisiert ist. Die Zugriffsberechtigung auf die redundanten Kommunikationskanäle KK_1, KK_2 wird nach einem statischen Zeitscheibenverfahren von der globalen Zeit abgeleitet. Das Zeitintervall, während dem jede Fehlertolerante Einheit FTE_1 FTE_2 FTE_3 FTE_4 mindestens einmal eine Sendezeitscheibe erhalten hat, bezeichnet man als Übertragungsrunde.

Da die Sendezeitpunkte jeder Nachricht a priori bekannt sind, kann in dieser neuen Kommunikationsarchitektur auch auf den Transport des Nachrichtennamens in der Nachricht verzichtet werden. Der Empfänger ist in der Lage aufgrund des Empfangszeitpunktes den Nachrichtennamen zu rekonstruieren. Dadurch ergibt sich eine wesentliche Reduktion der Nachrichtenlänge.

In der folgenden Beschreibung werden die Indizes 1, 2, 3, 4 zur Unterscheidung der einzelnen Fehlertoleranten Einheiten FTE der Übersicht halber weggelassen, da diese Einheiten im wesentlichen gleich aufgebaut sind.

Jede Kommunikationskontrolleinheit KE verfügt über einen inneren Zustand, der sich im konkreten Beispiel aus dem globalen Zeitfeld und einem 4 Bit langen Mitgliedsfeld zusammensetzt. Jedem der vier Fehlertoleranten Einheiten FTE ist ein bestimmtes Bit in diesem Mitgliedsfeld zugeordnet, dessen Zustand WAHR die Funktionstüchtigkeit und dessen Zustand FALSCH einen Fehlerzustand dieser Fehlertoleranten Einheit FTE aus der Sicht der betrachtenden Kommunikationskontrolleinheit KE zum Zeitpunkt der letzten global bekannten Sendezeitscheibe dieser Fehlertoleranten Einheit FTE darstellt.

Bei dem erfindungsgemäßen Verfahren wird prinzipiell zwischen zwei Nachrichtenarten unterschieden, den Initialisierungsnachrichten und den Standardnachrichten. Beide Nachrichtenarten beinhalten ein Kontrollfeld K, ein Datenfeld D und ein CRC (Cyclic Redundancy Check) Feld. Das Nachrichtenformat für das konkrete Ausführungsbeispiel ist

in Fig. 2 dargestellt. Das Kontrollfeld K hat eine Länge von 1 Byte. Das erste Bit des Kontrollfelds ist das Initialisierungsbit I. Die nächsten drei Bits sind die Betriebsänderungsbits B und die letzten vier Bits des Kontrollfelds sind Quittungsbits Q. Das Datenfeld D hat eine Länge von 8 Byte. Das CRC Feld hat eine Länge von 2 Byte.

Bei Initialiserungsnachrichten, die durch den Wert WAHR im ersten Bit I des Kontrollfelds gekennzeichnet sind und die im Datenfeld D den inneren Zustand der sendenden Kommunikationskontrolleinheit enthalten, wird der Inhalt des CRC Felds nach einem bekannten Verfahren (CCITT Standard: Data Transmission over the Telephone Network, Series V Recommendations, Session V41, The Orange Book, VIII.1, International Telecommunications Union, Geneva, 1977) über die Verkettung von Kontrollfeld K und Datenfeld D gebildet. Die Initialisierungsnachrichten werden zur Initialisierung des Systems und zur Reintegration von reparierten Computern benötigt. Im normalen Betrieb ist das Senden von Initialisierungsnachrichten nicht erforderlich. Die Initialisierungsnachrichten können im Hintergrund übertragen werden, wenn keine anderen Nachrichten zu senden sind.

Bei Standardnachrichten, die durch den Wert FALSCH im ersten Bit I des Kontrollfelds K gekennzeichnet sind, wird der Inhalt des CRC Felds bei der sendenden Kommunikationskontrolleinheit KE erfindungsgemäß über die Verkettung von Kontrollfeld K, Datenfeld D und dem lokalen inneren Zustand des Senders gebildet. Die empfangende Kommunikationskontrolleinheit KE kann durch die CRC-Überprüfung der Verkettung der ankommenden Nachricht mit ihrem lokalen inneren Zustand eine fehlerhafte Nachricht oder ein Abweichen der inneren Zustände von Empfänger und Sender erkennen. Um diese Zustandsgleichheit schnell, d.i. vor dem Senden der nächsten Nachricht, überprüfen zu können, ist das beschriebene CRC Verfahren vorteilhaft in der Hardware ausgeführt. Erfindungsgemäß kann durch diese Innovation die Gleichheit der Zustände zwischen Sender und Empfänger (damit wird eine indirekte Bestätigung des Nachrichtenempfangs realisiert) festgestellt werden, ohne die Zustandsinformation selbst in der Nachricht übertragen zu müssen. Dadurch ergibt sich in vorteilhafter Weise eine signifikante Reduktion der Nachrichtenlänge.

Bei einem weiteren, hier nicht näher erläuterten, Ausführungsbeispiel kann es vorteilhaft sein, den inneren Zustand durch zusätzliche Informationen, wie z.B. den momentanen Betriebszustand oder kryptographische Informationen, zu ergänzen, um auch die Gleichheit dieser zusätzlichen Informationen beim Sender und Empfänger durch das beschriebene innovative Verfahren überprüfen zu können. Verschiedenen

Betriebszuständen können unterschiedliche Nachrichtenformate und unterschiedliche Übertragungsrunden zugeordnet werden.

Wenn im Bit I, das zur Unterscheidung von Initialisierungsnachrichten und Standardnachrichten dient, ein Fehler auftritt, so wird durch die beschriebene Erfindung im Rahmen der CRC Überprüfung diese Nachricht als fehlerhaft erkannt und verworfen.

Eine empfangende Kommunikationskontrolleinheit KE kennzeichnet eine Fehlertolerante Einheit FTE in ihrem Mitgliedsfeld als fehlerhaft, wenn in der a priori bekannten Zeitscheibe dieser Fehlertoleranten Einheit FTE keine der erwarteten Nachrichten dieser Fehlertoleranten Einheit FTE mit korrektem CRC Feld bei der empfangenden Kommunikationskontrolleinheit KE eintrifft. Aufgrund des a priori Wissens über die Zeitscheiben des Senders kann der Empfänger zwei verschiedene Fehlerarten unterscheiden: keine Nachricht wurde empfangen oder eine Nachricht mit einem falschen Inhalt (fehlerhafter CRC check) wurde empfangen. Der Empfänger zählt mittels eines CRC-Fehlerzählers die seit seinem letzten Sendezeitpunkt empfangenen Nachrichten mit fehlerhaften CRC. Die seit seinem letzten Sendezeitpunkt empfangenen richtigen Nachrichten zählt der Empfänger in einem OK-Zähler.

Der entsprechend seinem lokalen Mitgliedsfeld erste aktive Nachfolger der sendenden Fehlertoleranten Einheit FTE quittiert in seinem Kontrollfeld die korrekt empfangenen Nachrichten der vorausgegangenen Fehlertoleranten Einheit FTE.

Unmittelbar vor dem Senden entscheidet eine Kommunikationskontrolleinheit, ob ihre Funktion fehlerhaft ist. Eine Kommunikationskontrolleinheit KE betrachtet sich dann als fehlerhaft, wenn

(1) einer ihrer Fehlererkennungsmechanismen einen Fehler anzeigt oder
(2) keine ihrer Nachrichten, die sie in ihrer letzten FTE Zeitscheibe gesendet hat, von einer der Kommunikationskontrolleinheiten KE der nachfolgenden Fehlertoleranten Einheit FTE quittiert wurde, oder
(3) der Inhalt ihres OK-Zählers kleiner ist als der Inhalt ihres CRC-Fehlerzählers.

Wenn sich eine Kommunikationskontrolleinheit KE als fehlerhaft einstuft, so sendet sie keine Nachricht, geht in einen Fehlerbehandlungszustand über und initialisiert einen Wiederanlauf.

Das beschriebene Verfahren funktioniert auch, wenn eine Kommunikationskontrolleinheit KE innerhalb einer Übertragungsrunde mehrfach aufscheint.

Die Kommunikationskontrolleinheit KE eines Schattencomputers SC erkennt aufgrund des Ausbleibens der Nachrichten der aktiven Computer AC ihrer Fehlertoleranten Einheit FTE,. daß diese Computer ausgefallen sind. In einem solchen Fall übernimmt die Kommunikationskontrolleinheit KE des Schattencomputers SC die Sendezeitscheibe des ausgefallenen Computers, um die Redundanz kurzfristig wieder herzustellen.

Aus dem Zeitintervall zwischen dem erwarteten und tatsächlichen Eintreffen einer Nachricht kann die Differenz der Uhrenstände zwischen Sender und Empfänger vom Empfänger berechnet werden. Erfindungsgemäß ist in diesem Kommunikationssystem kein expliziter Nachrichtenaustausch zur Uhrensynchronisation erforderlich. Dies führt zu einer wesentlichen Reduktion der Nachrichtenzahl.

Eine schnelle Reaktion bei Auftreten einer Notsituation wird erfindungsgemäß durch die Bereitstellung einer Anzahl von Betriebszustandsänderungsbits B im Kontrollfeld K jeder Nachricht realisiert. Im vorliegenden Beispiel sind drei solche Betriebszustandsänderungsbits B vorgesehen. Wenn eine Kommunikationskontrolleinheit KE eine schnelle Betriebszustandsänderung signalisieren muß, so kann sie das entsprechende Betriebszustandsänderungsbit B setzen. Spätestens innerhalb der nächsten Übertragungsrunde können dann alle anderen Computer auf die Betriebszustandsänderung reagieren.

Durch die beschriebene Erfindung kann die Effizienz der Kommunikation in Echtzeitsystemen wesentlich verbessert werden. Vergleicht man dieses innovative Verfahren mit den in der Literatur veröffentlichten Verfahren (1992 SAE Handbook, Vol, pp. 20.301-20.302, Society of Automotive Engineers, 400 Commonwealth Drive, Warrendale, Pa, USA), so ergibt sich gegenüber den bisher bekannten Verfahren J1850, CAN und Token Slot Network eine Ausweitung der Dienste und eine Verbesserung der Antwortzeiten um mehr als 50 %.

Zusammenfassend sei festgehalten, daß die folgenden innovativen Merkmale dieser Erfindung zu einer wesentlichen Reduktion der Nachrichtenlänge und der Nachrichtenzahl in einem Kommunikationssystem für eine Fehlertolerante verteilte Echtzeit-Computerarchitektur führen:

(1) Die Feststellung der Zustandsgleichheit zwischen Sender und Empfänger ohne Übertragung der Zustandsinformation durch Einbeziehung der Zustandsinformation in die CRC Berechnung.

(2) Die Elimination der Quittungsnachrichten durch Einführung eines kurzen Quittungsfeldes in jeder Nachricht.

(3) Die implizite Synchronisation der Uhren ohne Übertragung von Synchronisationsnachrichten.

(4) Die Ableitung des Nachrichtennamens aus den a priori bekannten Sende- und Empfangszeitpunkten einer Nachricht ohne den Nachrichtennamen explizit übertragen zu müssen.

(5) Die Bereitstellung eines Betriebszustandsänderungsfeldes in jeder Nachricht, um auf wichtige Betriebszustandsänderungen ohne zusätzlichen Nachrichtenaustausch schnell reagieren zu können.

(6) Die Auswertung der Verhältniszahl der mit richtigem und falschem CRC Feld eintreffenden Nachrichten, um ohne expliziten Nachrichtenaustausch feststellen zu können, ob sich ein Empfänger in der Mehrheit der funktionierenden Kommunikationseinheiten befindet.

Abschließend ist noch anzuführen, daß sich die Erfindung keineswegs auf die oben beschriebene Konfiguration mit vier Fehlertoleranten Einheiten FTE beschränkt, sondern mit jeder beliebigen Anzahl Fehlertoleranter Einheiten implementiert werden kann. Ebenso ist die Konfiguration einer Fehlertoleranten Einheit nicht auf zwei aktive Computer und einen Schattencomputer mit je einer Kommunikationskontrolleinheit mit zwei Ports und das Broadcastsystem nicht auf zwei Kommunikationskanäle beschränkt, sondern kann entsprechend der geforderten Redundanz völlig beliebig gewählt werden. Insbesondere können die Kommunikationskanäle auch als "on-board" oder "on-chip" Verbindungen ausgeführt sein.

PATENTANSPRÜCHE

1. Verfahren zur Übermittlung von Nachrichten innerhalb einer verteilten Echtzeit-Computerarchitektur mit einer gemeinsamen globalen Zeitbasis, bestehend aus einer Mehrzahl Fehlertoleranter Einheiten (FTE_1, FTE_2, FTE_3, FTE_4), welche zumindest je einen fail-silent Computer (AC_{1a}, AC_{1b}, SC_1, AC_{2a}, AC_{2b}, SC_2, AC_{3a}, AC_{3b}, SC_3, AC_{4a}, AC_{4b}, SC_4) und je Computer eine Kommunikationskontrolleinheit (KE_{1a}, KE_{1b}, KE_{1c}, KE_{2a}, KE_{2b}, KE_{2c}, KE_{3a}, KE_{3b}, KE_{3c}, KE_{4a}, KE_{4b}, KE_{4c}) mit zumindest einem Kommunikationsport aufweisen, wobei jede Fehlertolerante Einheit (FTE_1, FTE_2, FTE_3, FTE_4) über zumindest einen Kommunikationskanal (KK_1, KK_2) mit jeder anderen Fehlertoleranten Einheit (FTE_1, FTE_2, FTE_3, FTE_4) verbunden ist und der Zugriff auf den zumindest einen Kommunikationskanal (KK_1, KK_2) durch ein statisches, von der gemeinsamen globalen Zeitbasis abgeleitetes zyklisches Zeitscheibenverfahren erfolgt, **dadurch gekennzeichnet, daß** die zu übertragenden Nachrichten aus einem Kotrollfeld (K), einem Datenfeld (D) und einem CRC (Cyclic- Redundancy Check) Feld (CRC) zusammengesetzt sind, wobei das CRC-Feld von Standardnachrichten, welche durch ein bestimmtes Bit (I) des Kontrollfeldes (K) gekennzeichnet sind, aus der Verkettung des Kontrollfeldes (K), des Datenfeldes (D) und eines lokalen inneren Zustandes einer sendenden Kommunikationskontrolleinheit gebildet wird und sich der lokale innere Zustand einer solchen Kontrolleinheit aus der Verbindung der globalen Zeit mit einem Mitgliedsfeld ergibt, in welchem jeder Fehlertoleranten Einheit (FTE_1, FTE_2, FTE_3, FTE_4) ein bestimmtes Bit zugeordnet ist, dessen Zustand WAHR die Funktionstüchtigkeit und dessen Zustand FALSCH einen Fehlerzustand dieser Fehlertoleranten Einheit (FTE_1, FTE_2, FTE_3, FTE_4) anzeigt, sodaß eine empfangende Kommunikationskontrolleinheit durch Überprüfung einer einlangenden Nachricht sowohl eine fehlerhafte Nachricht, als auch ein Abweichen der inneren Zustände der sendenden und empfangenden Kommunikationskontrolleinheit erkennen kann.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, daß** die empfangende Kommunikationskontrolleinheit eine Fehlertolerante Einheit (FTE_1, FTE_2, FTE_3, FTE_4) durch Setzen des zugeordneten Bits im Mitgliedsfeld als fehlerhaft kennzeichnet, wenn im

Sendezeitintervall dieser Einheit keine der erwarteten Nachrichten mit einem korrekten CRC-Feld (CRC) eintrifft.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** das Kontrollfeld (K) als erstes Bit ein Initialisierungsbit () zur Unterscheidung zwischen Standard- und Initialisierungsnachrichten aufweist.

4. Verfahren nach Anspruch 3, **dadurch gekennzeichnet, daß** das Kontrollfeld (K) weiters eine Anzahl von Quittungsbits (Q) aufweist, mittels welchen der korrekte Empfang einer oder mehrerer vorangegangener Nachrichten quittiert wird, sodaß jede Kommunikationskontrolleinheit durch Überprüfung des Kontrollfeldes (K) bei Empfang einer Nachricht feststellen kann, ob alle ihre Kommunikationsports funktioniert haben und weiters aufgrund des Verhältnisses der Anzahl korrekt empfangener Nachrichten zu der Anzahl von Nachrichten mit CRC-Fehlern erkennen kann, ob sie sich in der Mehrheit der funktionierenden Kommunikationskontrolleinheiten befindet.

5. Verfahren nach Anspruch 3 oder 4, **dadurch gekennzeichnet, daß** das Kontrollfeld (K) weiters eine Anzahl von Betriebsartenänderungsbits (B) aufweist.

6. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, daß** der innere Zustand, der bei Bildung des CRC-Feldes von Standardnachrichten eingeschlossen und beim Empfänger überprüft wird, weiters ein Betriebsartenfeld umfaßt.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, daß** der Nachrichtenname aus dem a priori festgelegten Sendezeitpunkt einer Nachricht abgeleitet wird, sodaß dieser nicht im Nachrichteninhalt mitgeführt werden muß.

8. Verfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, daß** die Erstellung der globalen Zeitbasis dezentral in jeder Kommunikationskontrolleinheit erfolgt, wobei die Unterschiede der Uhrenstände zwischen den Fehlertoleranten Einheiten (FTE_1, FTE_2, FTE_3, FTE_4) aus den bekannten, statisch festgelegten Sendezeitpunkten und der lokalen Messung der Ankunftszeiten der erwarteten Nachrichten ermittelt werden.

9. Kommunikationskontrolleinheit zur Übermittlung von Nachrichten innerhalb einer verteilten Echtzeit- Computerarchitektur mit einer gemeinsamen globalen Zeitbasis, bestehend aus einer Mehrzahl Fehlertoleranter Einheiten (FTE_1, FTE_2, FTE_3, FTE_4), welche zumindest je einen fail-silent Computer (AC_{1a}, AC_{1b}, SC_1, AC_{2a}, AC_{2b}, SC_2, AC_{3a}, AC_{3b}, SC_3, AC_{4a}, AC_{4b}, SC_4) und je Computer eine solche

Kommunikationskontrolleinheit (KE_{1a}, KE_{1b}, KE_{1c}, KE_{2a}, KE_{2b}, KE_{2c}, KE_{3a}, KE_{3b}, KE_{3c}, KE_{4a}, KE_{4b}, KE_{4c}) mit zumindest einem Kommunikationsport aufweisen, wobei jede Fehlertolerante Einheit (FTE_1, FTE_2, FTE_3, FTE_4) über zumindest einen Kommunikationskanal (KK_1, KK_2) mit jeder anderen Fehlertoleranten Einheit (FTE_1, FTE_2, FTE_3, FTE_4) verbunden ist und der Zugriff auf den zumindest einen Kommunikationskanal (KK_1, KK_2) durch ein statisches, von der gemeinsamen globalen Zeitbasis abgeleitetes zyklisches Zeitscheibenverfahren erfolgt, **dadurch gekennzeichnet, daß** die Kommunikationskontrolleinheit dazu vorgesehen ist, die zu übertragenden Nachrichten aus einem Kotrollfeld (K), einem Datenfeld (D) und einem CRC (Cyclic-Redundancy Check) Feld (CRC) zusammenzusetzen, wobei das CRC-Feld von Standardnachrichten, welche durch ein bestimmtes Bit (I) des Kontrollfeldes (K) gekennzeichnet sind, aus der Verkettung des Kontrollfeldes (K), des Datenfeldes (D) und eines lokalen inneren Zustandes einer sendenden Kommunikationskontrolleinheit gebildet wird, und wobei die Kommunikationskontrolleinheit weiters dazu vorgesehen ist, ihren lokalen inneren Zustand aus der Verbindung der globalen Zeit mit einem Mitgliedsfeld zu erstellen, in welchem jeder Fehlertoleranten Einheit (FTE_1, FTE_2, FTE_3, FTE_4) ein bestimmtes Bit zugeordnet ist, dessen Zustand WAHR die Funktionstüchtigkeit und dessen Zustand FALSCH einen Fehlerzustand dieser Fehlertoleranten Einheit (FTE_1, FTE_2, FTE_3, FTE_4) anzeigt, sodaß eine empfangende Kommunikationskontrolleinheit durch Überprüfung einer einlangenden Nachricht sowohl eine fehlerhafte Nachricht, als auch ein Abweichen der inneren Zustände der sendenden und empfangenden Kommunikationskontrolleinheit erkennen kann.

10. Kommunikationskontrolleinheit nach Anspruch 9, **dadurch gekennzeichnet, daß** sie je einen Zähler zum Feststellen der Anzahl korrekt empfangener Nachrichten und einen Zähler zum Festellen der Anzahl empfangender Nachrichten mit CRC-Fehlern aufweist.

11. Kommunikationskontrolleinheit nach Anspruch 9 oder 10, **dadurch gekennzeichnet, daß** sie eine Logik aufweist, welche dazu geeignet ist, nach Empfang einer Nachricht eine Änderung der Betriebsart der Fehlertoleranten Einheit (FTE_1, FTE_2, FTE_3, FTE_4) herbeizuführen.

12. Kommunikationskontrolleinheit nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet, daß** sie eine Logik zum Feststellen der Ankunftszeit und zum Vergleich dieser Ankunftszeitpunkte mit den a priori festgelegten Sendzeitpunkten einer Nachricht aufweist.

13. Kommunikationskontrolleinheit nach einem der Ansprüche 9 bis 12, **dadurch gekennzeichnet, daß** sie als Singlechip Controller oder als Teil eines Singlechip Microcomputers realisiert ist.

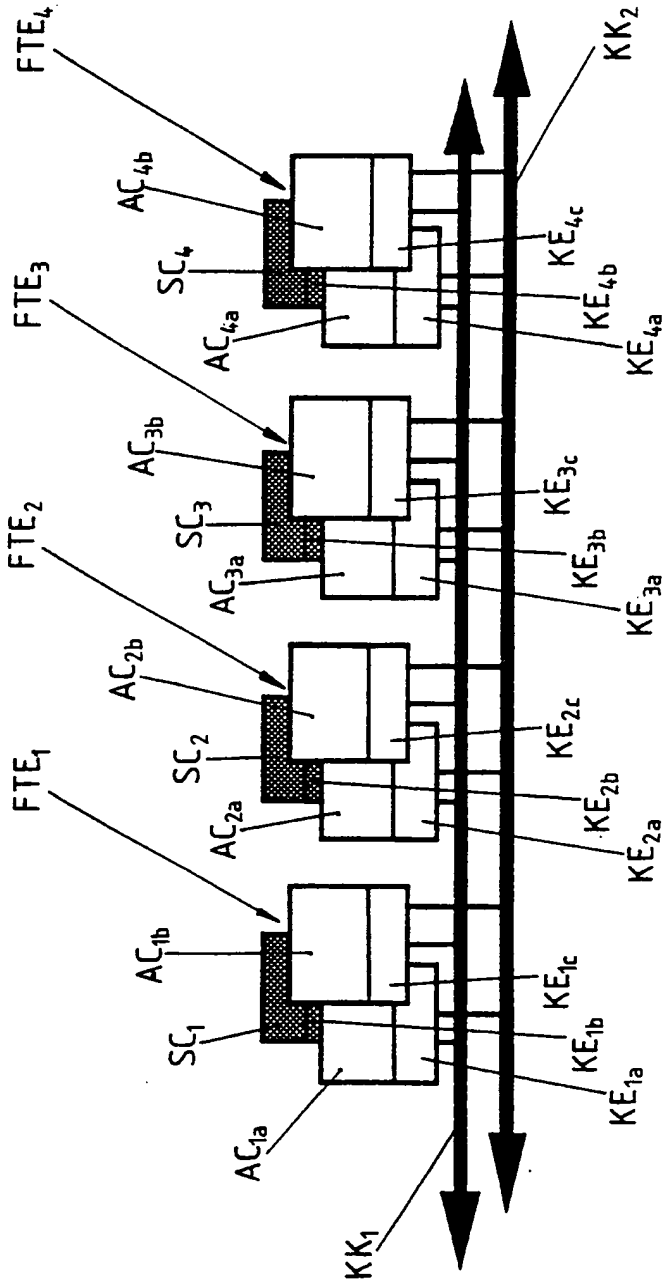

FTE4
FTE3
FTE2
FTE1
AC4b
SC4
AC4a
AC3b
SC3
AC3a
AC2b
SC2
AC2a
AC1b
SC1
AC1a
KK2
KK1
KE4c
KE4b
KE4a
KE3c
KE3b
KE3a
KE2c
KE2b
KE2a
KE1c
KE1b
KE1a

FIG.1

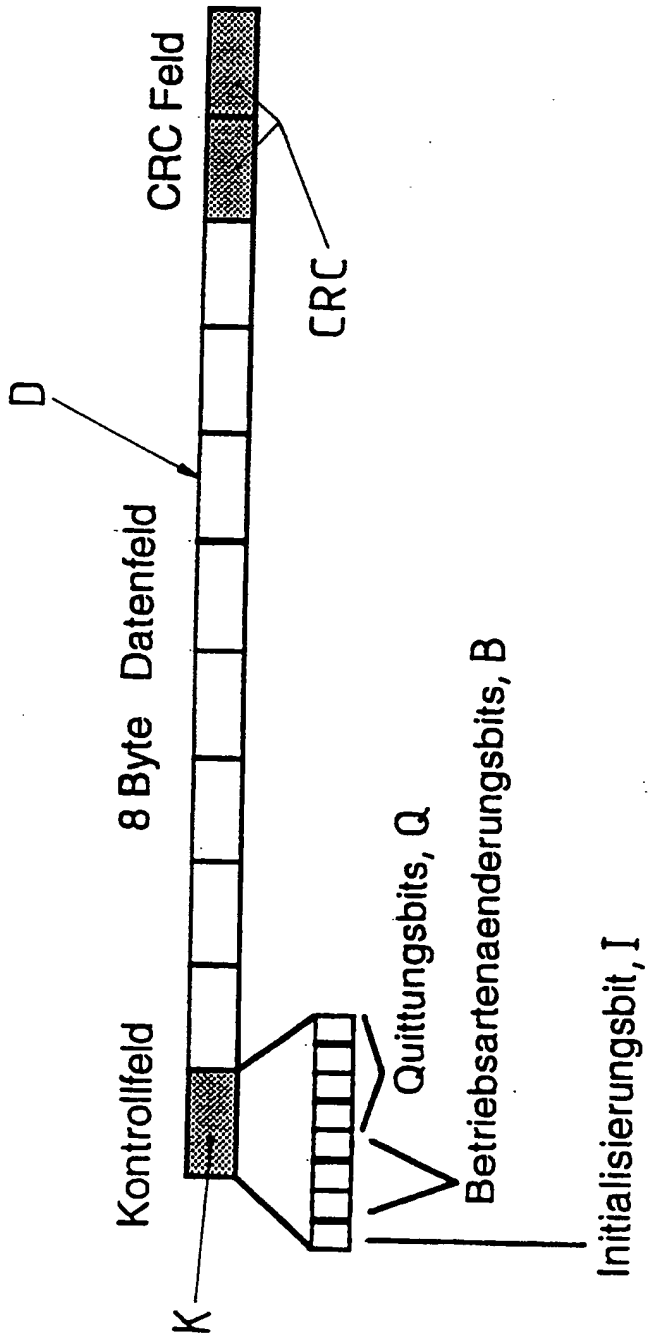

CRC Feld
CRC
D
8 Byte Datenfeld
Kontrollfeld
K
Quittungsbits, Q
Betriebsartenaenderungsbits, B
Initialisierungsbit, I

FIG.2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AT 93/00138

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.[5] G06F11/08 G06F11/10 G06F11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl.[5] G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A, 4 860 006 (BARALL) 22 August 1989 see the abstract; claim 1; fig. 2,3,5,6	1,9
A	EP,A,0 033 228 (FORNEY INTERNATIONAL) 5 August 1981 see the abstract; claims 1,2; fig. 5-8	1,9

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 December 1993 (01.12.93)	22 December 1993 (22.12.93)
Name and mailing address of the ISA/ EUROPEAN PATENT OFFICE Facsimile No.	Authorized officer Telephone No.